Раздел V

Вопросы образования в области информационной безопасности

УДК 004.056.53

С.М. Климов[1,2], М.П. Сычёв[1]
[1]Россия, Москва, МГТУ им. Н.Э.Баумана
[2]Россия, Королёв, 4 ЦНИИ Минобороны России

СТЕНДОВЫЙ ПОЛИГОН УЧЕБНО-ТРЕНИРОВОЧНЫХ И ИСПЫТАТЕЛЬНЫХ СРЕДСТВ В ОБЛАСТИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Статья посвящена эмпирическому подходу к оценке реального уровня защищенности и устойчивости функционирования критически важных информационных объектов путем испытаний их сегментов на стендовом полигоне в условиях компьютерных атак, информационной нагрузки и в процессе выполнения технологического цикла управления.

Критически важный информационный объект; компьютерная атака; стендовый полигон учебно-тренировочных и испытательных средств.

S.M. Klimov[1,2], M.P. Sychjov[1]
[1]Russia, Moscow, MSTU N.E. Bauman
[2]Russia, Korolev, Central Research Institute of the Russian Defense Ministry 4

POSTER POLYGON FOR TRAINING AND TESTING FACILITIES IN THE FIELD OF INFORMATION SECURITY

The article is devoted to the empirical approach to the assessment of the real level of security and sustainability of mission-critical information objects by testing their segments on the bench in a range of computer attacks, information load and during the execution of the process control loop.

Critical information object; computer attack; poster landfill of training and testing tools.

Стендовый полигон учебно-тренировочных и испытательных средств в области обеспечения информационной безопасности представляет собой совокупность аппаратно-программных комплексов имитации сегментов критически важных информационных объектов (КВИО), компьютерных атак, средств противодействия компьютерным атакам и средств оценки защищенности и устойчивости функционирования в составе замкнутой локальной вычислительной сети [1].

Предлагаемый стендовый полигон путем масштабирования структуры, модернизации элементов, настройки специального программного обеспечения и использования технологий виртуализации может использоваться для решения комплекса задачв области обеспечения информационной безопасности:

1.Обучения специалистов в области информационной безопасности.

2.Тренировки подразделений информационной безопасности и руководящего состава организаций (не специалистов в области информационной безопасности) действиям в условиях применения нарушителем массированных компьютерных атак на средства автоматизации систем связи, транспорта, управления, навигации и других КВИО.

3.Испытаний сегментов КВИО в условиях компьютерных атак, информационной нагрузки и в процессе выполнения технологического цикла управления для оценки их реального уровня защищенности и устойчивости функционирования.

Типовую структуру стендового полигона учебно-тренировочных и испытательных средств в области информационной безопасности предлагается сформировать по модульному принципу в виде совокупности базовых и специальных аппаратно-программных комплексов, взаимоувязанных по функциям и формату данных (рис. 1).

Первый модуль – система имитаторов информационно-технических воздействий и сценариев действий нарушителя.

Второй модуль – сегменты КВИО, включающие в свой состав, как элементы автоматизированных систем, так и компьютеризированных и роботизированных образцов.

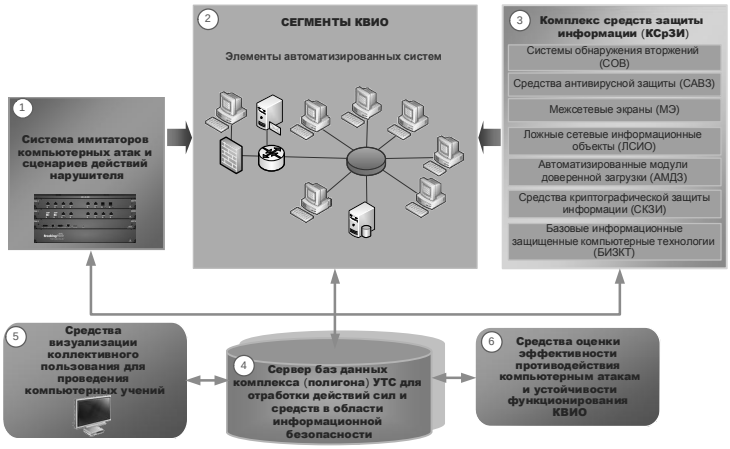

Рис. 1. – Типовая структура стендового полигона учебно-тренировочных и испытательных средств в области информационной безопасности

Третий модуль – комплекс средств защиты информации.

Четвертый модуль – сервер баз данных комплекса (полигона) УТС для отработки действий сил и средств в области информационной безопасности.

Пятый модуль – средства визуализации коллективного пользования для проведения компьютерных учений.

Шестой модуль – средства оценки эффективности противодействия компьютерным атакам и устойчивости функционирования КВИО.

Под устойчивостью функционирования КВИО будем понимать его способность обеспечивать установленные регламенты выполнения технологических циклов управления в условиях компьютерных атак.

Типовой сценарий нарушения устойчивости функционирования КВИО (рис. 2), на которых осуществляются выполнение технологических циклов сбора, обработки, передачи и выдачи управляющей информации, показывает, что в усло-

виях компьютерных атак параметры объекта выходят за допустимые пределы, что приводит к нарушению его функционирования.

Сущность нарушения устойчивости функционирования КВИО в условиях компьютерных атак заключается в том, что несвоевременно выполняется технологические циклы управления (ТЦУ). Вводится искусственное замедление. На период времени действия компьютерных атак и восстановления КВИО срываются сроки обработки и передачи требуемых объемов информации или данные поступают в искаженном виде. Таким образом, для КВИО главное это фактор времени выполнения требуемого объема информационно-расчетных задач и выдачи управляющих воздействий.

В докладе более подробно рассмотрена задача испытаний сегментов КВИО в условиях компьютерных атак, информационной нагрузки и в процессе выполнения технологического цикла управления для оценки их реального уровня защищенности и устойчивости функционирования.

Эмпирический подход к оценке реального уровня защищенности и устойчивости функционирования КВИО заключается в том, что на стендовом полигоне моделируется (имитационно или натурно) реальный технологический цикл управления (ТЦУ) объекта, в ходе выполнения которого, через потенциальные уязвимые места по модели нарушителя (внешнего и внутреннего), реализуются воздействия: компьютерные атаки и информационная нагрузка.

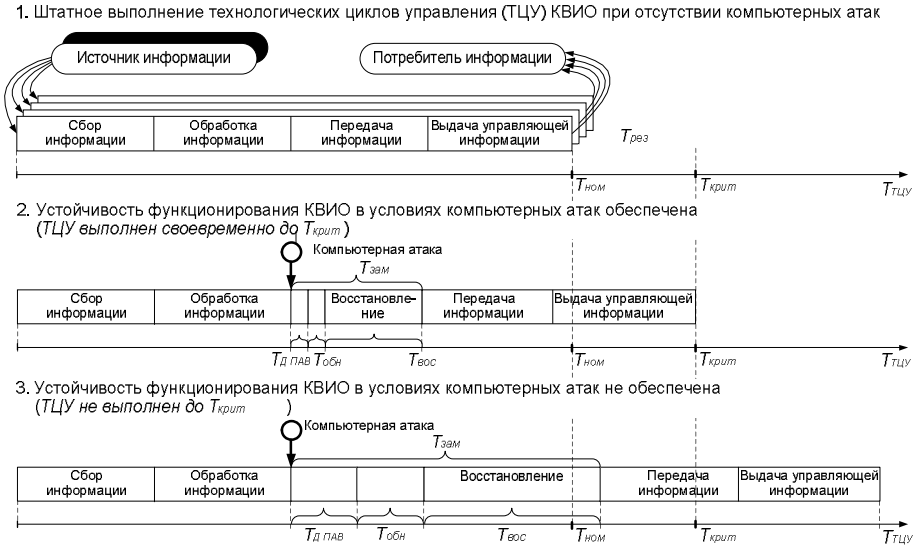

Рис. 2. – Типовой сценарий нарушения устойчивости функционирования КВИО в условиях компьютерных атак

Современные компьютерные атаки могут быть реализованы и сымитированы следующими основными способами:

- реализация компьютерных атак (программ эксплойтов) на выявленные уязвимости (IP и MAC-адреса и доступные порты) – распределенный «отказ в обслуживании» (DDoS-атака);
- реализация потока стандартных и нестандартных протоколов передачи данных на сетевые устройства с целью выявления неизвестных уязвимостей (метод фаззинга);

- реализация интенсивной информационной нагрузки в виде пакетов данные на доступные сетевые адреса;
- скрытое проникновение, самораспространение и самомодификация вредоносного кода неизвестных атак (атак нулевого дня или «0-days» - атак) в КВИО по типу «ботсетей» с целью сбора информации и дальнейшего функционального поражения этой сети.

Сущность испытаний сегментов КВИО в условиях компьютерных атак на стендовом полигоне – провести оценку эффективности как существующего комплекса средств защиты информации (КрСЗИ), так и прогнозные исследования прототипов перспективных КВИО в защищенном исполнении для оценки их вероятностно-временных характеристик в условиях компьютерных атак.

Экспериментальные исследования на стендовом полигоне проводятся с использованием макетов аппаратно-программных комплексов имитатора компьютерных атак, средств предупреждения и обнаружения компьютерных атак и средств оценки эффективности противодействия компьютерным атакам.

Испытания сегментов КВИО в условиях компьютерных атак осуществляются в следующей последовательности:

- оценка эффективности компьютерных атак нарушителя;
- оценка эффективности средств противодействия компьютерным атакам;
- оценка эффективности активного противодействия источникам компьютерным атакам;
- оценка устойчивости функционирования КВИО в условиях воздействия компьютерных атак.

В ходе реализации модели угроз компьютерных атак на КВИО на стендовом полигоне важно развернуть систему зарубежных и отечественных имитаторов компьютерных атак.

Имитатор компьютерных атак BreakingPointфирмы IXIA позволяет реализовывать более 34000 DDoS атак, генерируемых из базы атак на потенциальные уязвимости по классификации CWE. Далее проводится сравнительный анализ легитимного и вредоносного трафика и оценка статистики успешно реализованных атак. Кроме того, другим средством имитации программно-аппаратных воздействий методом фаззинга является комплекс программ Defensics. Данный комплекс позволяет имитировать потоки более 200 протоколов передачи данных, выявлять уязвимости и получать статистические данные для подготовки мер по повышению защищенности тестируемых устройств.

В качестве прототипа отечественных средств имитации компьютерных атак на КВИО можно рассмотреть комплекс «Биоцикл», который позволяет осуществлять имитацию пассивного и активного сканирования сетей, компьютерных атак через цифровые каналы связи (проводные, волоконно-оптические и цифровые радиосети) при отработке возможных действий нарушителей и специалистов в области обеспечения информационной безопасности.

Стендовый полигон информационной безопасности в 4 ЦНИИ (рис. 3) с аппаратно-программными средствами моделирования и обнаружения компьютерных атак на КВИО, позволяют:

- испытать сегменты КВИО различного применения в условиях компьютерных атак;
- отработать средства обнаружения, предупреждения и ликвидации последствий компьютерных атак;
- реализовать и апробировать систему оповещения органов управления об компьютерных атаках;
- сформировать базу данных результатов испытаний КВИО и КСрЗИ.

Средства стендового полигона для мониторинга защищенности сетей спутниковой связи в условиях компьютерных атак позволяют в зоне обслуживания космического аппарата связи проводить технический анализ широкополосных спутниковых сигналов в различных диапазонах частот и оценивать защищенность спутникового абонентского оборудования, управляющих станций и потребительского сегмента сети спутниковой связи в условиях потенциальных воздействий.

В настоящее время стендовые полигоны развернуты в ряде высших учебных заведений, которые также могут использоваться для испытаний КВИО в форме имитационных процессов функционирования сегментов реальных автоматизированных систем, КСрЗИ и средств реализации компьютерных атак.

Рис3. – Стендовый полигон информационной безопасности в 4 ЦНИИ

В интересах подготовки специалистов федеральных органов исполнительной власти в области защиты информации развернут учебно-испытательный стенд МГТУ им. Н.Э.Баумана (рис. 4). Он позволяет комплексно готовить специалистов по защите от утечки по техническим каналам связи, противодействию компьютерным атакам, доверенным программно-аппаратным средам и особенностям выявления и защиты от информационно-психологических воздействий.

Хорошим развитием рассмотренных стендовых полигонов информационной безопасности является то, что их наращивание позволит сформировать базовое ядро стенда в области информационной безопасности для ряда Федеральных органов исполнительной власти.

Спецификой средств испытаний ряда КВИО в условиях компьютерных атак является то обстоятельство, что для подобных исследований необходимо развертывать стенды из функциональных эквивалентов реальных средств (например, средств передачи данных по цифровым каналам связи) и натурно моделировать процессы управления.

В том случае, когда реализовать стендовый полигон реального сегмента КВИО проблематично, дорого и необходимо отработать сложные сценарии, хорошим выходом являются компьютерные игры оценки устойчивости функционирования и уровня защиты информации.

Рис. 4. – Учебно-испытательный стенд МГТУ им. Н.Э.Баумана в области защиты информации

В настоящее время завершается разработка новой версии специального программного обеспечения компьютерной игры в области информационной безопасности – «Кристалл». Главным критерием оценки в данной игре это обеспечение игроком в роли администратора безопасности своевременности выполнения ТЦУ в структуре КВИО в условиях компьютерных атак. Данная игра в форме двусторонних, компьютерных, имитационных моделей позволяет:

- практически обучать специалистов по защите информации анализу сценариев нарушителя по реализации компьютерных атак;
- приобретать навыки выявления уязвимых мест;
- противодействовать компьютерным атакам на основе применения КСрЗИ и средств восстановления КВИО;
- в тестовом режиме проверять знания руководящих документов по защите информации;
- логике применения средств маршрутизации сети и защиты информации.

На рис. 5 представлен интерфейс игры для нарушителя, который в игровой форме готовит и реализует сценарии типовых компьютерных атак на уязвимые места КВИО.

Рис. 6 демонстрирует возможности игрока в роли администратора безопасности информации по реализации функций противодействия компьютерных атак на основе применения КСрЗИ и выполнению ТЦУ КВИО за установленное время.

Определение победителя в компьютерной игре «Кристалл» осуществляется по времени выполнения ТЦУ КВИО и бальной системе с учетом знаний и практических навыков обучаемого в динамике игры.

Таким образом, создание стендового полигона учебно-тренировочных и испытательных средств в области обеспечения информационной безопасности, позволит в ходе испытаний оценить вероятностно-временные характеристики КВИО и встроенные КСрЗИ в условиях имитации реальных компьютерных атак и ТЦУ, а также в ходе этих испытаний обучить специалистов практическим навыкам по противодействию компьютерным атакам.

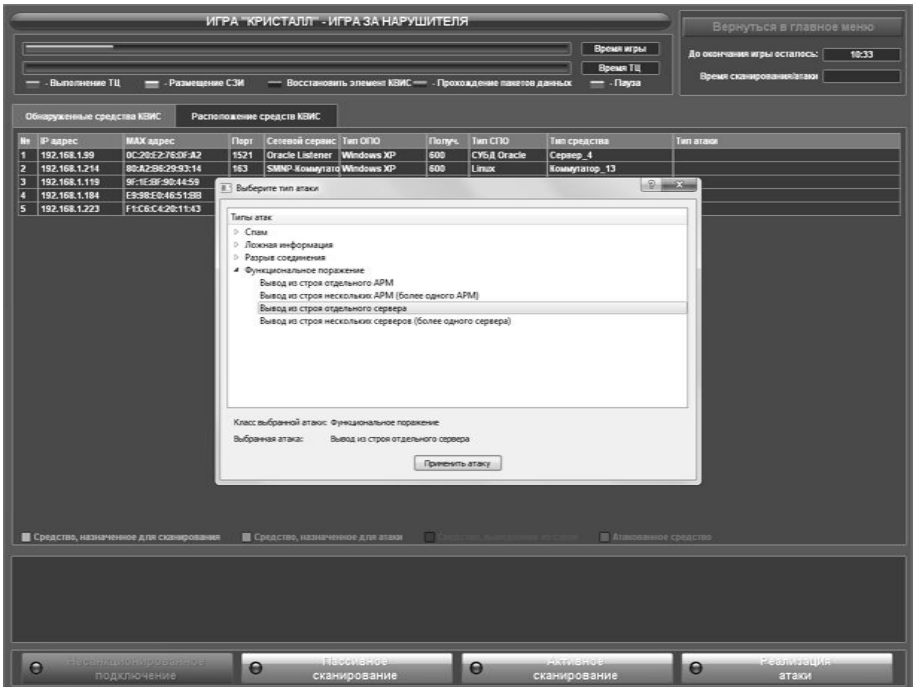

Рис. 5. – Интерфейс игры для нарушителябезопасности информации

Рис. 6. – Интерфейс обучаемого (игрока) в роли администратора безопасности информации

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1.*Климов С.М.* Методы и модели противодействия компьютерным атакам. Люберцы:КАТАЛИТ, 2008. – 316 с.

УДК 004.056(075.8)

А.П.Алексеев, М.И.Макаров, В.В.Орлов
Россия, Самара, Поволжский государственный университет телекоммуникаций и информатики

ТРЕБОВАНИЯ К УЧЕБНОЙ ЛИТЕРАТУРЕ ПО ЗАЩИТЕ ИНФОРМАЦИИ

В докладе рассмотрены требования к учебным пособиям по криптографии и стеганографии, а также принципы построения современных систем защиты информации.

Рассмотренымногоуровневые системы защиты информации, которые включают в себя криптографический, алгоритмический, стеганографический барьеры, пространственное распыление и временное разделение. Описывается способ скрытой передачи информации в сетевых пакетах.

Криптография; стеганография; контейнер; пространственно-временное распыление.

A.P. Alekseev, M.I. Makarov, V.V. Orlov
Russia, Samara, Volga State University of Telecommunications and Informatics

REQUIREMENTS FOR EDUCATIONAL LITERATURE FOR THE PROTECTION OF INFORMATION

The report examines the requirements for textbooks on cryptography and steganography, as well as the principles of modern systems of information protection.

Considers multi-level information security system, which includes a cryptographic algorithmic, steganography barriers, the spatial and temporal separation spray. It describes a method for secure data transmission in network packets.

Cryptography; steganography; container; Spatial and temporal spray.

Число публикаций, посвящённых криптографии и стеганографии, растёт экспоненциально. По криптографии издано большое число учебников, задачников, пособий для проведения лабораторных работ и практических занятий [1, 2, 12, 13], а также проводятся онлайн курсы [10, 11]. Применительно к стеганографии заметен дефицит учебной литературы, содержащей описание лабораторных работ и практических задач. Компенсировать это пробел пытаются преподаватели и учёные в различных высших учебных заведениях, в том числе России и Болгарии. В России такими работами являются [3, 4, 5], а в Болгарии – книги, написанные профессором С. Станевым и его учениками [6, 14, 15].

Авторы данного доклада придерживаются мнения, что современная учебная литература по защите информации должна строиться на основе комплексного многоуровневого подхода. Это означает, в частности, что методы стеганографии невозможно рассматривать изолированно от криптографии. В свою очередь, рассмотрение только лишь криптографических алгоритмов защиты данных не рас-